CLAIMS:

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

Sub A1

1. A system for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said system comprising:

means for determining fulfillment of one or more certain conditions at said destination location; and,

control means responsive to detection of a fulfilled one or more certain conditions for enabling access to content provided in a communicated package, whereby said access includes enabling a user to perform an operation on said package content at said destination location.

2. The system as claimed in Claim 1, wherein said electronic information packages include content comprising one or more of: e-mail messages, audio data, video data, animation data, textual data, and pictorial data.

3. The system as claimed in Claim 2, further including means for automatically destroying a received electronic information

package in response to detection of a fulfilled one or more certain conditions.

4. The system as claimed in Claim 3, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals, said system further comprising means for determining elapsed time from receipt of an electronic information package, said means generating a signal for destroying the received electronic information package after a time interval has elapsed.

5. The system as claimed in Claim 4, wherein said elapsed time interval is specified by a sender at said sending device, said electronic information package further comprising a specification of one or more time-out intervals for use by said elapsed timing means.

6. The system as claimed in Claim 5, wherein said operations enabled to be performed on said package content at said destination device include displaying one or more of video data, text, picture and animation data via a display device at said destination location.

7. The system as claimed in Claim 5, wherein said operations enabled to be performed on said package content at said destination device include playing audio data on one or several speakers at said destination location.

8. The system as claimed in Claim 3, wherein said access includes forbidding a user to perform an operation on said package content at said destination device, said operations that are forbidden to be performed on received information packages include one or more of: saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

9. The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting an attempted performance of a forbidden operation at the destination location, said destroying means automatically destroying a received electronic information package in response to said detection.

10. The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said

destination device further includes means for receiving a direct command signal from a sender at a sending device, said sender command triggering destruction of said electronic information package.

11. The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, said destroying means automatically destroying a received electronic information package in response to said detection.

12. The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting a second or repeated attempted to play or display information package content, said destroying means automatically destroying a received electronic information package in response to said detection.

13. The system as claimed in Claim 9, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

14. The system as claimed in Claim 9, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting a pressing of a key on a keyboard operable for said destination device.

15. The system as claimed in Claim 1, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying a user at said destination location for which access to these information packages is allowed.

16. The system as claimed in Claim 15, wherein said identification means includes video camera system for generating video signals at said destination device and a display device for receiving and displaying video signals at said sending device, said video camera system enabling a sender at a sending device to observe users attempting to read or play information package content at a destination device.

17. The system as claimed in claim 15, wherein said identification means for identifying a user at said destination location comprises:

means for enabling users to present a password to said system; and,

verification means for verifying a user's password prior to enabling access to said information package.

18. The system as claimed in Claim 15, wherein said identification means for identifying a user at said destination location comprises means for enabling users to present a data for authentification/verification that include one or more of the following: biometrics, fingerprint, and voice data.

19. The system as claimed in Claim 1, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying an electronic system at said destination location for which access to these information packages is allowed.

20. The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises a communication process that supports transferring electronic package content via a communication channel to new destination locations.

21. The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises an automated process capable of understanding information package content and performing necessary operations as required for playing said content.

22. The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises a robotic device.

23. The system as claimed in Claim 1, wherein said electronic information packages communicated from a sending device to a device at one or more destination locations, is communicated over a communications channel including one or more of: telephone wires, wireless channels, radio links, network data connection.

24. A method for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method comprising:

determining fulfillment of one or more conditions at said destination location; and,

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

25. The method as claimed in Claim 24, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

26. The method as claimed in Claim 25, wherein a fulfilled one or more certain condition includes detection of one or more

elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

27. The method as claimed in Claim 26, further including the step of enabling a sender to specify said time interval.

28. The method as claimed in Claim 24, wherein said step of enabling access to said content of said communicated package includes enabling a user to display one or more of video data, text, picture and animation data via a display device at said destination location, and play audio data on one or several speakers at said destination location.

29. The method as claimed in Claim 28, wherein said step of enabling access to said content of said communicated package includes forbidding a user to perform an operation on said package content at said destination device, said operations forbidden to be performed on received information packages

including one or more of: saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

30. The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location; and, in response to said detecting, automatically destroying a received electronic information package.

31. The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

32. The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination

locations, said physical hardware devices including CPU, memory or peripherals at said destination device, and in response to said detecting, automatically destroying a received electronic information package.

33. The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

34. The method as claimed in Claim 30, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

35. The method as claimed in Claim 30, wherein said step of detecting an attempted performance of a forbidden operation at

the destination location includes: detecting a pressing of a key on a keyboard operable for said destination device.

36. The method as claimed in Claim 24, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of: identifying a user at said destination location for which access to these information packages is allowed.

37. The method as claimed in Claim 36, wherein said identifying step includes implementing video camera device for generating video signals at said destination device for receipt by said sender, said sender receiving and displaying video signals at said sending device for identifying users attempting to read or play information package content at a destination device.

38. The method as claimed in Claim 37, wherein said identifying step further includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

39. The method as claimed in Claim 37, wherein said identifying step further includes authentificating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.

40. The method as claimed in Claim 24, wherein said step of determining fulfillment of one or more conditions at said destination location includes identifying an electronic system at said destination location for which access to these information packages is allowed.

41. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method steps comprising:

determining fulfillment of one or more conditions at said destination location; and,

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

42. The program storage device as claimed in Claim 41, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

43. The program storage device as claimed in Claim 42, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

44. The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location;

and, in response to said detecting, automatically destroying a received electronic information package.

45. The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

46. The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, and in response to said detecting, automatically destroying a received electronic information package.

47. The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

48. The program storage device as claimed in Claim 43, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

49. The program storage device as claimed in Claim 43, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting a pressing of a key on a keyboard operable for said destination device.

50. The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of: identifying a user at said destination location for which access to these information packages is allowed.

51. The program storage device as claimed in Claim 50, wherein said identifying step includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

52. The program storage device as claimed in Claim 50, wherein said identifying step includes authenticating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.